20

CLAIMS

What is claimed is:

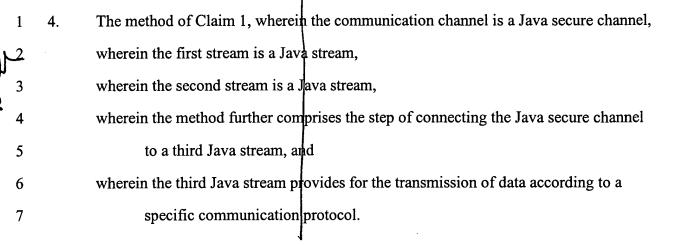
		1
1	1.	A method for providing communication protocol-independent security for data
2		transmitted between a first process, executing on a first network node, and a second
3		process, executing on a second network node, wherein the first network node and the
4		second network node each support at least one common communication protocol, the
5		method comprising the steps of:
6		a) establishing a communication channel between the first network node and the
7		second network node;
8		b) establishing a first stream between the first process and the communication
9		channel;
10		c) establishing a second stream between the second process and the communication
11		channel;
12		d) encrypting data to be transmitted between the first and second processes, the
13		encrypting of the data being independent of the at least one communication
14		protocol supported by the first network node;
15		e) writing the encrypted data to the first stream;
16		f) causing the encrypted data to be transmitted from the first network node to the
17		second network node;
18		g) reading the encrypted data from the second stream; and
19		h) decrypting the encrypted data to obtain decrypted data which is identical to the
20		data on the first network node before the data was encrypted.
		· · · · · · · · · · · · · · · · · · ·

comprises the step of reading the encrypted data from the second Java stream.

1	1	2.	The method of Claim 1, further including the steps of
D.	2		a) performing a communication protocol-specific encryption of the data on the first
cont	3		network node, and
v	4		b) performing a communication protocol-specific decryption of the data on the
	5		second network node.
	1	3.	The method of Claim 1, wherein the communication channel is a Java secure channel,
	2		wherein the first stream is a first Java stream,
			wherein the second stream is a second Java stream,
		2	wherein the step of establishing a communication channel between the first and
QT W	54	5	second network nodes further compreses the step of establishing a Java secure
	6		channel between the first and second network nodes,
	7		wherein the step of establishing a first stream between the first process and the
	8		communication channel further comprises the step of establishing a first Java
ī.	9		stream between the first process and the Java secure channel,
e e e e e e e e e e e e e e e e e e e	10		wherein the step of establishing a second stream between the second process and the
in the second	11		communication channel further comprises the step of establishing a second
	12		Java stream between the second process and the Java secure channel,
	13		wherein the step of writing the encrypted data to the first stream further comprises the
	14		step of writing the encrypted data to the first Java stream, and
	15		wherein the step of reading the encrypted data from the second stream further

16

5.



A computer-readable medium having stored thereon a plurality of sequences of instructions for providing communication protocol-independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol, the plurality of sequences of instructions including sequences of instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

- a) establishing a communication channel between the first network node and the second network node;
- b) establishing a first stream between the first process and the communication channel;
- c) establishing a second stream between the second process and the communication channel;
- d) encrypting data to be transmitted between the first and second processes, the encrypting of the data being independent of the communication protocols supported by the first network node;

ode to the
ode to the
tical to the
able medium
a on the first
a on the
a first Java
a first Java
a first Java first and
a first Java first and
a first Java first and a Java secure
a first Java first and a Java secure
a first Java first and a Java secure
a first Java first and a Java secure and the ng a first Java

wherein the step of writing the encrypted data to the first stream further comprises the step of writing the encrypted data to the first Java stream, and wherein the step of reading the encrypted data from the second stream further comprises the step of reading the encrypted data from the second Java stream.

8. The computer-readable medium of Claim 5, wherein the communication channel is a Java secure channel, wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the computer-readable medium further includes instructions for connecting the Java secure channel to a third Java stream, and wherein the third Java stream provides for the transmission of data according to a specific communication protocol.

- A communication network providing communication protocol-independent secure communication between a first network node and a second network node, wherein the first network node and the second network node each support at least one common communication protocol, wherein the first network node is communicatively coupled to the second network node by a communication channel, the communication network comprising:
 - a) a first process executing on the first network node, wherein the first process provides for the communication protocol-independent encryption of data;
 - b) a first stream which provides for the transfer of encrypted data between the first process and the communication channel;
 - c) a second process executing on the second network node; and

5

6

7

8

1

2

6

8

9

10

11

9.

1

2

3

5

6

7

8

9

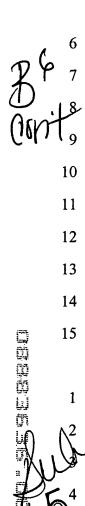
10

13.



- d) a second stream which provides for the transfer of encrypted data between the communication channel and the second process, wherein the second process also provides for the decryption of data which has been encrypted by the first process.
- 1 10. The communication network of Claim 9, wherein the second process further includes
 2 the capability to decrypt data based upon any communication protocol supported by
 3 the second network node.
- 1 11. The communication network of Claim 9, wherein the communication channel is a
 2 Java secure channel, the first stream is a Java stream and the second stream is a Java
 3 stream.
- 1 12. The communication network of Claim 11, further comprising a third Java stream
 2 connected to the Java secure channel, the third Java stream providing for the
 3 transmission of data according to a specific communication protocol.
 - A computer data signal embodied in a carrier wave and representing sequences of instruction which, when executed by one or more processors, provide communication protocol-independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol by performing the steps of:
 - a) establishing a communication channel between the first network node and the second network node;
 - b) establishing a first stream between the first process and the communication channel;

1,40



wherein the step of establishing a first stream between the first process and the communication channel further comprises the step of establishing a first Java stream between the first process and the Java secure channel, wherein the step of establishing a second stream between the second process and the

communication channel further comprises the step of establishing a second
Java stream between the second process and the Java secure channel,
wherein the step of writing the encrypted data to the first stream further comprises the
step of writing the encrypted data to the first Java stream, and
wherein the step of reading the encrypted data from the second stream further
comprises the step of reading the encrypted data from the second Java stream.

The computer data signal of Claim 3, wherein the communication channel is a Java secure channel,

wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the computer sequence of instructions further includes instructions for connecting the Java secure channel to a third Java stream, and wherein the third Java stream provides for the transmission of data according to a specific communication protocol.

8

6

7

16.

17. A method for providing communication protocol-independent security for data transmitted by a process executing on a network node, the method comprising the steps of:

- a) establishing a stream between the process and a communication channel;
- b) encrypting data to be transmitted by the process, the encrypting of the data being independent of a communication protocol supported by the network node;

 $\begin{cases} 1 \\ 2 \\ 3 \\ 4 \end{cases}$

5

6

3070-004/P2145/TJC

n 1	7	c) writing the encrypted data to the stream; and
	8	d) causing the encrypted data to be transmitted from the network node to the
	9	communication channel.
h	,	
	H 18.	The method of Claim 17, wherein the communication channel is a Java secure
	2	channel,
	3	wherein the stream is a first Java stream,
	4	wherein the step of establishing a stream between the process and the communication
	5	channel further comprises the step of establishing a Java stream between the
	6	process and the Java secure channel, and
	7	wherein the step of writing the encrypted data to the stream further comprises the step
	8	of writing the encrypted data to the Java stream.
IJ		1
Ui n	1 19.	The method of Claim 17, wherein the communication channel is a Java secure
	2	channel, wherein the stream is a Java stream,
		wherein the method further comprises the step of connecting the Java secure channel
	A)	to a second Java stream, and
ل	5	wherein the second Java stream provides for the transmission of data according to a
	6	specific communication protocol.
\.		
nd		
7946		